TAKATOSHI ONO
82478-4800
JOSEPH W. PRICE 949 253-4920

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年　１月２８日

出 願 番 号
Application Number: 特願２００３－０１８７６０

[ST. 10/C]: [ＪＰ２００３－０１８７６０]

出 願 人
Applicant(s): 松下電器産業株式会社

２００３年１０月１０日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫

出証番号　出証特２００３－３０８３７９７

【書類名】　特許願
【整理番号】　2968150001
【提出日】　平成15年 1月28日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/00　340
H04L 9/00
G06F 11/00　350
G09C 1/00　650
【発明者】
【住所又は居所】　愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
【氏名】　小野　貴敏
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　松崎　なつめ
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄
【選任した代理人】
【識別番号】　100103355
【弁理士】
【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　故障利用攻撃に対応した楕円曲線暗号装置および楕円べき倍演算装置

【特許請求の範囲】

【請求項１】　素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2 = x^3 + a \times x + b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋから、べき倍点ｋＱを求める楕円べき倍演算装置であって、

点Ｑの座標（Ｑｘ，Ｑｙ）と、べき倍係数ｋを入力する第一の入力手段と、

楕円曲線のパラメータである零次項係数ｂを入力する第二の入力手段と、

楕円曲線のパラメータである一次項係数ａを固定値として保持する楕円係数保持手段と、

前記第一の入力手段で入力された各値と、前記楕円係数保持手段で保持している一次項係数ａから、前記べき倍点ｋＱを求めるべき倍演算手段と、

前記第二の入力手段で入力された零次項係数ｂと、前記楕円係数保持手段で保持している一次項係数ａを用いて、前記べき倍演算手段によって求められた前記べき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定する判定手段と、

前記判定手段で前記べき倍点ｋＱの座標が楕円曲線上に存在すると判定された時のみ、前記べき倍演算手段で求められた前記べき倍点ｋＱを出力する出力手段とを備えたことを特徴とする楕円べき倍演算装置。

【請求項２】　前記楕円係数保持手段の代わりに、楕円曲線のパラメータである一次項係数ａを入力する第三の入力手段を備え、

前記べき倍演算手段は、前記楕円係数保持手段で保持している一次項係数ａの代わりに、前記第三の入力手段で入力された一次項係数ａを用いてべき倍点ｋＱを求め、

前記判定手段は、前記楕円係数保持手段で保持している一次項係数ａの代わりに、前記第三の入力手段で入力された一次項係数ａを用いてべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを特徴とする請求項１に記載の楕円べき倍演算装置。

【請求項３】　前記第二の入力手段の代わりに、前記第一の入力手段によって

入力された点Ｑの座標、並びに前記楕円係数保持手段で保持、もしくは前記第三の入力手段で入力された一次項係数ａから、零次項係数ｂを求める零次項係数演算手段を備え、

前記判定手段は、前記第二の入力手段で入力された零次項係数ｂの代わりに、零次項係数演算手段で求められた零次項係数ｂを用いてべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを特徴とする請求項１または２記載の楕円べき倍演算装置。

【請求項４】　前記判定手段によって楕円曲線上に存在しないと判定された時、その旨を出力するエラー出力手段をさらに備えたことを特徴とする請求項１から３のいずれか１項に記載の楕円べき倍演算装置。

【請求項５】　楕円曲線暗号を用いて、平文の暗号化処理、暗号文の復号化処理、平文に対する署名文の生成処理、平文と署名文に対する署名文の検証処理、署名文からの平文回復処理のいずれか若しくは前記各処理の複数処理を行う楕円曲線暗号装置であって、

前記各処理に用いる楕円べき倍演算処理に、請求項１から請求項４に記載の楕円べき倍演算装置を用いることを特徴とする楕円曲線暗号装置。

【請求項６】　素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋから、べき倍点ｋＱを求める楕円べき倍演算方法であって、

点Ｑの座標（Ｑｘ，Ｑｙ）とべき倍係数ｋを入力する第一の入力ステップと、

楕円曲線のパラメータである零次項係数ｂを入力する第二の入力ステップと、

楕円曲線のパラメータである一次項係数ａを固定値として保持する楕円係数保持ステップと、

前記第一の入力ステップで入力された各値と前記楕円係数保持ステップで保持している一次項係数ａから前記べき倍点ｋＱを求めるべき倍演算ステップと、

前記第二の入力ステップで入力された零次項係数ｂと前記楕円係数保持ステップで保持している一次項係数ａを用いて前記べき倍演算ステップによって求められた前記べき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定する判定ステップと、

前記判定ステップで前記べき倍点ｋＱの座標が楕円曲線上に存在すると判定された時のみ、前記べき倍演算ステップで求められた前記べき倍点ｋＱを出力する出力ステップとを備えたことを特徴とする楕円べき倍演算方法。

【請求項７】　前記楕円係数保持ステップの代わりに、楕円曲線のパラメータである一次項係数ａを入力する第三の入力ステップを備え、

前記べき倍演算ステップは、前記楕円係数保持ステップで保持している一次項係数ａの代わりに、前記第三の入力ステップで入力された一次項係数ａを用いてべき倍点ｋＱを求め、

前記判定ステップは、前記楕円係数保持ステップで保持している一次項係数ａの代わりに、前記第三の入力手段で入力された一次項係数ａを用いて前記べき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを特徴とする請求項６に記載の楕円べき倍演算方法。

【請求項８】　前記第二の入力ステップの代わりに、前記第一の入力ステップによって入力された点Ｑの座標、並びに前記楕円係数保持ステップで保持、もしくは前記第三の入力ステップで入力された一次項係数ａから、零次項係数ｂを求める零次項係数演算ステップを備え、

前記判定ステップは、前記第二の入力ステップで入力された零次項係数ｂの代わりに、零次項係数演算ステップで求められた零次項係数ｂを用いてべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを特徴とする請求項６または７記載の楕円べき倍演算方法。

【請求項９】　前記判定ステップによって楕円曲線上に存在しないと判定された時、その旨を出力するエラー出力ステップをさらに備えたことを特徴とする請求項６から８のいずれか１項に記載の楕円べき倍演算方法。

【請求項１０】　楕円曲線暗号を用いて、平文の暗号化処理、暗号文の復号化処理、平文に対する署名文の生成処理、平文と署名文に対する署名文の検証処理、署名文からの平文回復処理のいずれか若しくは前記各処理の複数処理を行う楕円曲線暗号方法であって、

前記各処理に用いる楕円べき倍演算処理に、請求項６から請求項９のいずれか１項に記載の楕円べき倍演算方法を用いることを特徴とする楕円曲線暗号方法。

【請求項１１】　コンピュータに、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋから、べき倍点ｋＱを求めさせる楕円べき倍演算プログラムであって、

点Ｑの座標（Ｑｘ，Ｑｙ）と、べき倍係数ｋを入力する第一の入力ステップと、

楕円曲線のパラメータである零次項係数ｂを入力する第二の入力ステップと、

楕円曲線のパラメータである一次項係数ａを固定値として保持する楕円係数保持ステップと、

前記第一の入力ステップで入力された各値と前記楕円係数保持ステップで保持している一次項係数ａから前記べき倍点ｋＱを求めるべき倍演算ステップと、

前記第二の入力ステップで入力された零次項係数ｂと前記楕円係数保持ステップで保持している一次項係数ａを用いて前記べき倍演算ステップによって求められた前記べき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定する判定ステップと、

前記判定ステップでべき前記倍点ｋＱの座標が楕円曲線上に存在すると判定された時のみ、前記べき倍演算ステップで求められた前記べき倍点ｋＱを出力する出力ステップとを実行させるための楕円べき倍演算プログラム。

【請求項１２】　前記楕円係数保持ステップの代わりに楕円曲線のパラメータである一次項係数ａを入力する第三の入力ステップを実行させ、

前記べき倍演算ステップは前記楕円係数保持ステップで保持している一次項係数ａの代わりに前記第三の入力ステップで入力された一次項係数ａを用いてべき倍点ｋＱを求めることを実行させ、

前記判定ステップは前記楕円係数保持ステップで保持している一次項係数ａの代わりに前記第三の入力手段で入力された一次項係数ａを用いて前記べき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを実行させる請求項１１に記載の楕円べき倍演算プログラム。

【請求項１３】　前記第二の入力ステップの代わりに、前記第一の入力ステップによって入力された点Ｑの座標、並びに前記楕円係数保持ステップで保持、も

しくは前記第三の入力ステップで入力された一次項係数ａから、零次項係数ｂを求める零次項係数演算ステップを実行させ、

前記判定ステップは、前記第二の入力ステップで入力された零次項係数ｂの代わりに、零次項係数演算ステップで求められた零次項係数ｂを用いてべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定することを実行させる請求項１１または１２記載の楕円べき倍演算プログラム。

【請求項１４】　前記判定ステップによって楕円曲線上に存在しないと判定された時その旨を出力するエラー出力ステップをさらに実行させる請求項１１から１３のいずれか１項に記載の楕円べき倍演算プログラム。

【請求項１５】　楕円曲線暗号を用いて、コンピュータに、平文の暗号化、暗号文の復号化、平文に対する署名文の生成、平文と署名文に対する署名文の検証、もしくは署名文からの平文回復のいずれか、もしくは前記各処理の複数を行う楕円曲線暗号プログラムであって、

前記各処理に用いる楕円べき倍演算処理に、請求項１１から請求項１４のいずれか１項に記載の楕円べき倍演算プログラムを用いる楕円曲線暗号プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は故障利用攻撃に対応する楕円曲線暗号装置及びその方法に関する。

【０００２】

【従来の技術】

従来、情報の秘匿認証等を実現する手段として公開鍵暗号法が知られている。公開鍵暗号法では、自分のみが保持する秘密鍵と、それに対応し公開する公開鍵のペアが生成され、各種処理が行われる。図１は、公開鍵暗号法を用いたメッセージの暗号化通信の一例を示している。メッセージ送信装置１０１は入力されたメッセージを暗号化し、メッセージ受信装置１０２に送信する。メッセージ受信装置１０２はメッセージ送信装置１０１から送られてきた暗号化メッセージを受信し、復号したメッセージを出力する。公開鍵１０３は、メッセージ受信装置１０２の持つ秘密鍵１０４に対応しており、メッセージの暗号化に用いられる。秘

密鍵１０４はメッセージ受信装置１０２が秘密裏に持ち、暗号化メッセージの復号に用いられる。

【０００３】

公開鍵暗号法は、処理時間が大きいという欠点はあるものの、秘密鍵を複数で共有する必要がないことから高セキュリティを必要とする場合に良く用いられており、一般に良く知られている公開鍵暗号法としては、ＲＳＡ暗号と楕円曲線暗号が存在する。

【０００４】

公開鍵暗号法では、秘密鍵をＩＣカードなど外部に漏れない手段を用いて保持するのが一般的であるが、近年、外部に出力される様々な情報からそれら秘密情報を解析する方法が知られるようになってきた。その一つに故障利用攻撃（ＤＦＡ攻撃ともいう）が存在する。

【０００５】

故障利用攻撃では、暗号処理を行っている間に過電流などを用い故意に故障を誘発する。そして故障を起こす時点までに演算された値を出力値として得る。こうして得られた出力値を多数集めることによって、秘密情報を少しずつ解析する攻撃法である。

【０００６】

図２は秘密鍵を内蔵するＩＣカードに対する故障利用攻撃の概念図である。故障利用攻撃の対象となるＩＣカード２０１は、内部に秘密鍵２０２を保持する。秘密鍵２０２はＩＣカード２０１内部の演算でのみ使用され外部に出力されることはない。正規の入力データ２０３は例えば認証用データなどがこれにあたる。出力データ２０４は例えば認証用データの署名データなどがこれにあたる。スパーク電流２０５は、故意にＩＣカード２０１の演算に故障を誘発させ、出力データ２０４を正規の演算結果ではなく、演算途中の値とさせるものである。

【０００７】

図３に従来知られている故障利用攻撃のフローチャートを示す。不正データの取得（ステップ３０１）は、正規データ入力（ステップ３０１ａ）、故障誘発（ステップ３０１ｂ）、演算途中結果の取得（ステップ３０１ｃ）から成る。

【０００８】

故障誘発（ステップ３０１ｂ）では、スパーク電流などを発生時刻を変化させておこし、様々な時点での演算途中結果を不正データとして取得する。３０１ａ、３０１ｂ、３０１ｃの各ステップは、多数の不正データを取得するため繰り返し行われる。

【０００９】

こうして取得した多数の演算途中結果を解析することで（ステップ３０２）秘密情報（秘密鍵）を計算する。

【００１０】

一般に故障利用攻撃に対応する方法としては、演算結果を公開情報によって演算前の値に戻す計算が行われ、正しく元の値に戻された時のみ出力を行うという方法が取られる。

【００１１】

またＲＳＡ暗号に対する故障利用攻撃に対応する方法としては、演算途中の結果に対しエラー検出フラグも同時に計算、保持し、演算結果出力直前に前記エラー検出フラグを検証しているものもある（例えば、特許文献１参照）。

【００１２】

また楕円曲線暗号の場合、使用する楕円曲線が固定であるということを利用して、演算結果が固定の楕円曲線上に存在するか否かを判定してから出力を行うという方法も取られる。

【００１３】

図４は故障利用攻撃に対する対策を行っていない楕円べき倍演算装置の構成例である。一般に楕円曲線暗号装置では、内部に楕円べき倍演算部を持ち、そこで秘密鍵による演算を行っている。従って以降楕円べき倍演算部から成る楕円べき倍演算装置での故障利用攻撃に焦点を置いて説明する。

【００１４】

べき倍係数入力部４０１は楕円べき倍演算に用いるべき倍係数を入力する。このべき倍係数値として秘密鍵値が用いられる場合がある。被演算値入力部４０２は、被べき倍点を入力する。

【００１５】

なお、ここでは入力された被べき倍点が楕円曲線上に存在するという前提になっている。

【００１６】

一次項保持部４０３は、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$における一次項係数ａを保持する。楕円べき倍演算部４０４は、べき倍係数入力部４０１で入力されたべき倍係数、被演算値入力部４０２で入力された被演算点、一次項保持部４０３で保持されている一次項係数ａを用いて、楕円べき倍演算を行う。演算結果出力部４０５は、楕円べき倍演算部４０４で演算された楕円べき倍点を値として出力する。前述した通り図４の楕円べき倍演算装置では故障利用攻撃に対する対策を行っていないため、楕円べき倍演算部４０４で演算途中の値を演算結果としてしまっても、そのまま演算結果出力部４０５で外部出力されてしまう。

【００１７】

図５は従来知られている故障利用攻撃に対する対策を施した楕円べき倍演算装置の構成例である。図４の基本構成に、零次項保持部５０１と演算結果検証部５０２が追加されている。

【００１８】

零次項保持部５０１は、楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$における零次項係数ｂを保持する。演算結果検証部５０２は、楕円べき倍演算部４０４で演算された楕円べき倍点を、一次項保持部４０３で保持していた一次項、並びに零次項保持部５０１で保持していた零次項を用いて、楕円曲線状の点であるか否かを検証する。演算結果出力部４０５は、演算結果検証部５０２で正しいと検証された時のみ演算した楕円べき倍点を値として出力する。その結果、たとえべき倍演算部４０４で演算途中の結果を演算結果としてしまっても、演算結果検証部５０２で検証失敗となるため、外部出力はされない構成となっている。ただしこの構成では常に同じ零次項保持部の値を用いるため、零次項を固定した固定楕円曲線での楕円べき倍演算のみ可能となる。

【００１９】

【特許文献１】

特開平１１－８６１６号公報

【００２０】

【発明が解決しようとする課題】

前記従来の方法によれば、楕円べき倍演算装置を故障利用攻撃に対応させるには、使用する楕円曲線を固定する必要があった。しかし楕円曲線を固定すると、零次項ｂを変化させることによって異なる暗号となる楕円曲線暗号の汎用性が阻害されるという課題があった。

【００２１】

【課題を解決するための手段】

上記課題を解決するために、本発明に係る楕円べき倍演算装置は、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋから、べき倍点ｋＱを求める楕円べき倍演算装置であって、点Ｑの座標（Ｑｘ，Ｑｙ）と、べき倍係数ｋを入力する第一の入力手段と、楕円曲線のパラメータである零次項係数ｂを入力する第二の入力手段と、楕円曲線のパラメータである一次項係数ａを固定値として保持する楕円係数保持手段と、前記第一の入力手段で入力された各値と、前記楕円係数保持手段で保持している一次項係数ａから、べき倍点ｋＱを求めるべき倍演算手段と、前記第二の入力手段で入力された零次項係数ｂと、前記楕円係数保持手段で保持している一次項係数ａを用いて、前記べき倍演算手段によって求められたべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定する判定手段と、前記判定手段でべき倍点ｋＱの座標が楕円曲線上に存在すると判定された時のみ、前記べき倍演算手段で求められたべき倍点ｋＱを出力する出力手段とを備えたことを特徴とする。

【００２２】

また上記課題を解決するために、本発明に係る楕円べき倍演算装置は、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋが与えられ、べき倍点ｋＱを求める楕円べき倍演算装置であって、前記第二の入力手段の代わりに、点

Ｑの座標、一次項係数ａから、零次項係数ｂを求める零次項係数演算手段を備え、前記判定手段は、前記第二の入力手段で入力された零次項係数ｂの代わりに、零次項係数演算手段で求められた零次項係数ｂを用い、その他の手段は前記したものと同じ処理を行うことを特徴とする。

【００２３】

また上記課題を解決するために、本発明に係る楕円曲線暗号装置は、楕円曲線暗号を用いて、平文の暗号化、暗号文の復号化、平文に対する署名文の生成、平文と署名文に対する署名文の検証、もしくは署名文からの平文回復のいずれか、もしくは前記各処理の複数を行う楕円曲線暗号装置であって、前記各処理に用いる楕円べき倍演算処理に、前記楕円べき倍演算装置を用いることを特徴とする。

【００２４】

上記課題を解決するために、本発明に係る楕円べき倍演算方法は、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋから、べき倍点ｋＱを求める楕円べき倍演算方法であって、点Ｑの座標（Ｑｘ，Ｑｙ）と、べき倍係数ｋを入力する第一の入力ステップと、楕円曲線のパラメータである零次項係数ｂを入力する第二の入力ステップと、楕円曲線のパラメータである一次項係数ａを固定値として保持する楕円係数保持ステップと、前記第一の入力ステップで入力された各値と、前記楕円係数保持ステップで保持している一次項係数ａから、べき倍点ｋＱを求めるべき倍演算ステップと、前記第二の入力ステップで入力された零次項係数ｂと、前記楕円係数保持ステップで保持している一次項係数ａを用いて、前記べき倍演算ステップによって求められたべき倍点ｋＱの座標が楕円曲線上に存在するか否かを判定する判定ステップと、前記判定ステップでべき倍点ｋＱの座標が楕円曲線上に存在すると判定された時のみ、前記べき倍演算ステップで求められたべき倍点ｋＱを出力する出力ステップとを備えたことを特徴とする。

【００２５】

また上記課題を解決するために、本発明に係る楕円べき倍演算方法は、素数ｐを用いた剰余体Ｆｐ上に定義された楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$において、楕円曲線上の任意の点Ｑとｐ未満の正の整数ｋが与えられ、べき倍点

ｋＱを求める楕円べき倍演算方法であって、前記第二の入力ステップの代わりに、点Ｑの座標、一次項係数ａから、零次項係数ｂを求める零次項係数演算ステップを備え、前記判定ステップは、前記第二の入力ステップで入力された零次項係数ｂの代わりに、零次項係数演算ステップで求められた零次項係数ｂを用い、その他のステップは前記したものと同じ処理を行うことを特徴とする。

【００２６】

また上記課題を解決するために、本発明に係る楕円曲線暗号方法は、楕円曲線暗号を用いて、平文の暗号化処理、暗号文の復号化処理、平文に対する署名文の生成処理、平文と署名文に対する署名文の検証処理、署名文からの平文回復処理のいずれか若しくは前記各処理の複数処理を行う楕円曲線暗号方法であって、前記各処理に用いる楕円べき倍演算処理に、前記楕円べき倍演算方法を用いることを特徴とする。

【００２７】

【発明の実施の形態】

図６は本発明における楕円べき倍演算装置の構成図である。

【００２８】

零次項入力部６０１は、楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$における零次項係数ｂを入力する。零次項保持部５０１は、固定の値ではなく零次項入力部６０１で入力された値を保持する。

【００２９】

図７は、本発明における楕円べき倍演算装置の別の構成図である。

【００３０】

零次項演算部７０１は、被演算値入力部４０２で入力された被べき倍点と一次項保持部４０３で保持されている楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$における一次項係数ａを用い、零次項係数ｂを演算する。被べき倍点の座標を（Ｘ，Ｙ）とすると、$Y^2-X^3-a\times X$の値がｂとなる。零次項保持部５０１は零次項演算部７０１で演算された値を保持する。

【００３１】

図８は、図７に構成例を示した楕円べき倍演算装置で用いられる、本発明にお

ける楕円べき倍演算方法のフローチャートである。最初にべき倍係数ｋ、並びに被べき倍点Ｑ＝（Ｘ，Ｙ）の入力を行う（ステップ８０１）。次に保持領域に保持されている楕円曲線Ｅ（Ｆｐ）：$y^2=x^3+a\times x+b$における一次項係数ａとステップ８０１で入力された被べき倍点Ｑを用いて、零次項係数ｂを計算する（ステップ８０２）。計算されたｂの値は一次項係数ａと共に保持領域に保持する。次にべき倍点ｋＱを演算する（ステップ８０３）。そしてべき倍点ｋＱの検証を行う（ステップ８０４）。検証の際に保持領域に保持されている一次項係数ａ、並びに零次項係数ｂを用いる。検証に成功した場合のみ次のステップに移行する（ステップ８０５）。最後にべき倍点ｋＱの出力を行う（ステップ８０６）。

【００３２】

べき倍点の検証に失敗した際には、失敗した旨を知らせるエラー出力を行っても良いし、演算結果を何も出力しないようにしても良い。また楕円曲線の一次項係数は－３という値を取ると高速な楕円べき倍演算を行うことができることが知られているため、この実施の形態では固定値として保持するようにしたが、べき倍係数などと同様外部から入力する構成としても良い。

【００３３】

【発明の効果】

以上のように本発明によれば、楕円曲線を固定することなく故障利用攻撃に対応した楕円べき倍演算を行うことができる。従って、従来の楕円曲線を固定して故障利用攻撃に対応した楕円べき倍演算装置に比べ、汎用性が高くなり、様々な用途に同一の装置を用いることができる。

【００３４】

さらに、べき倍係数ｋと被べき倍点Ｑの入力のみで、楕円曲線を固定せず故障利用攻撃に対応した楕円べき倍演算を行うことができる。従って、従来の楕円べき倍演算装置と入出力方法を変えることなく、汎用性を保ったまま故障利用攻撃に対応できるようになる。

【図面の簡単な説明】

【図１】

従来技術の公開鍵暗号法を用いたメッセージの暗号化通信の例を示す概念図

【図２】

従来知られているＩＣカードに対する故障利用攻撃の概念図

【図３】

従来知られている故障利用攻撃のフローチャート

【図４】

従来技術の故障利用攻撃に対応していない楕円べき倍演算装置の機能ブロック図

【図５】

従来技術の故障利用攻撃に対応した楕円べき倍演算装置の機能ブロック図

【図６】

本発明の実施の形態である故障利用攻撃に対応した楕円べき倍演算装置の機能ブロック図

【図７】

本発明の実施の形態である故障利用攻撃に対応した楕円べき倍演算装置の別の機能ブロック図

【図８】

本発明の実施の形態である故障利用攻撃に対応した楕円べき倍演算方法のフローチャート

【符号の説明】

４０１　べき倍係数入力部

４０２　被演算値入力部

４０３　一次項保持部

４０４　楕円べき倍演算部

４０５　演算結果出力部

５０１　零次項保持部

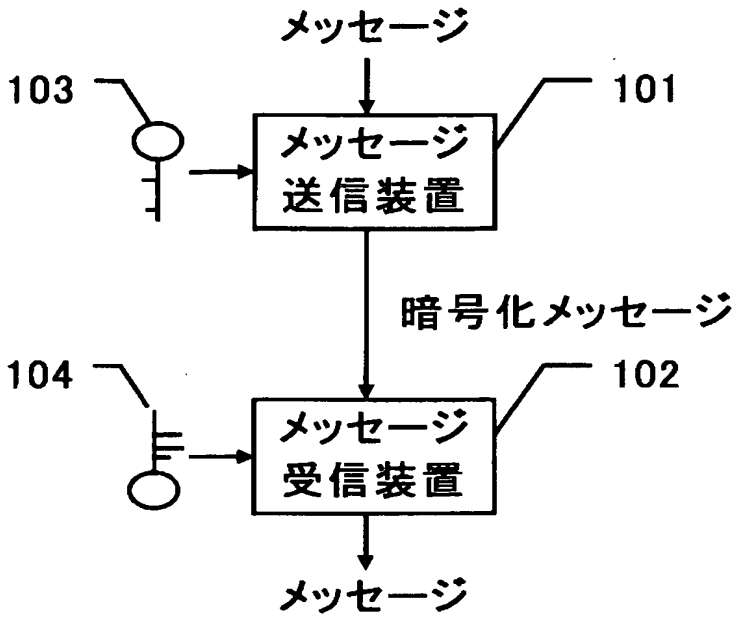
５０２　演算結果検証部

６０１　零次項入力部

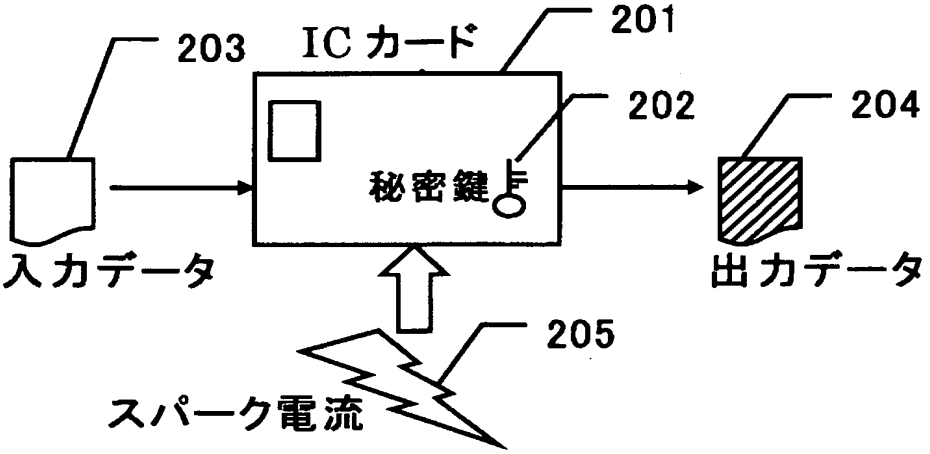
７０１　零次項演算部

【書類名】　図面

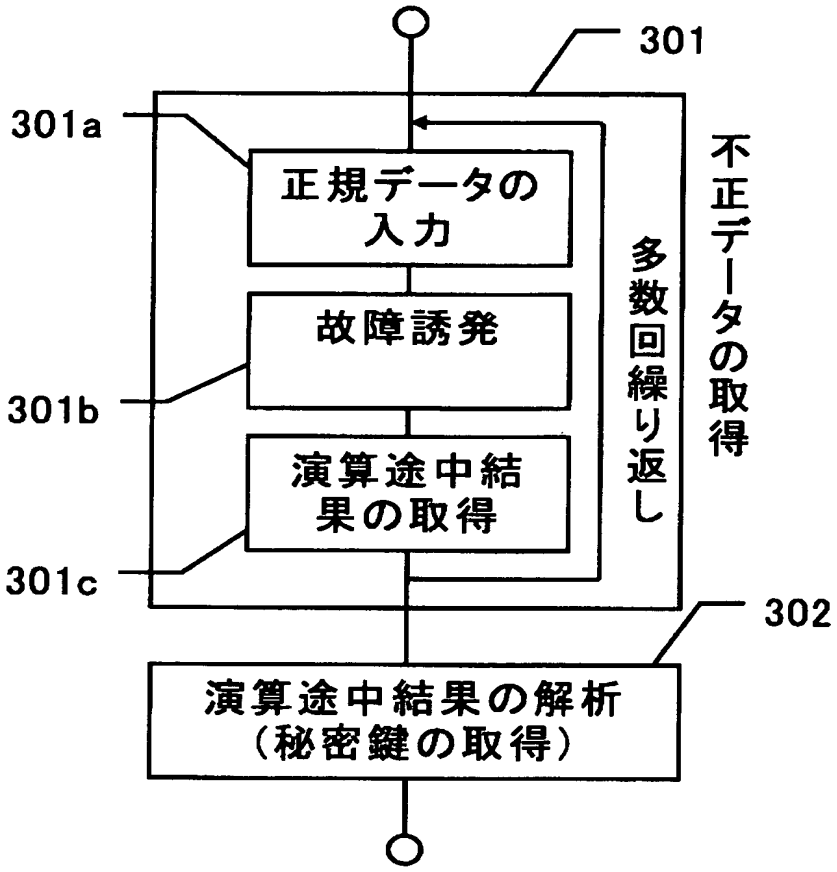
【図１】


メッセージ
103
101
メッセージ
送信装置
暗号化メッセージ
104
102
メッセージ
受信装置
メッセージ

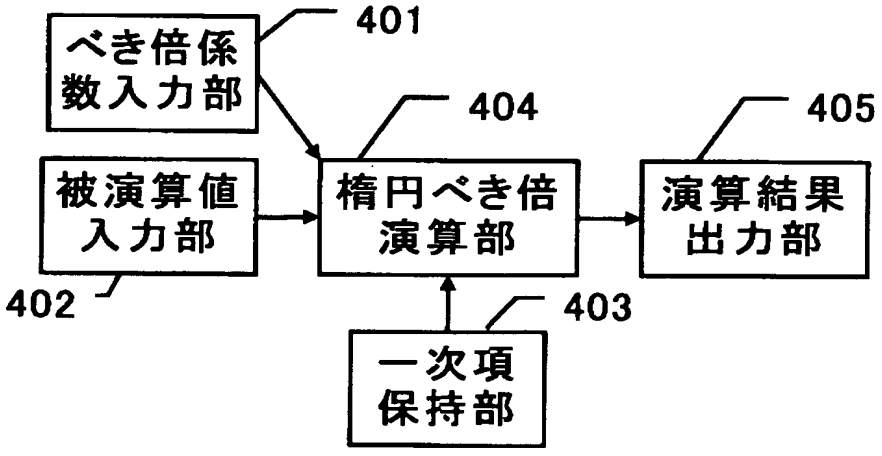
【図２】


203
ICカード
201
202
204
秘密鍵
入力データ
出力データ
205
スパーク電流

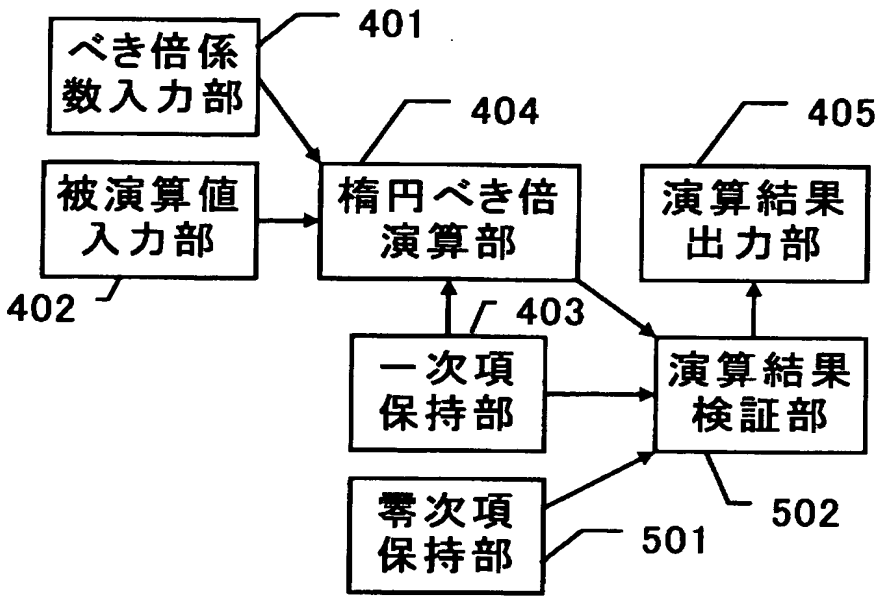
【図３】


301
301a
正規データの入力
故障誘発
301b
演算途中結果の取得
301c
多数回繰り返し
不正データの取得
302
演算途中結果の解析（秘密鍵の取得）

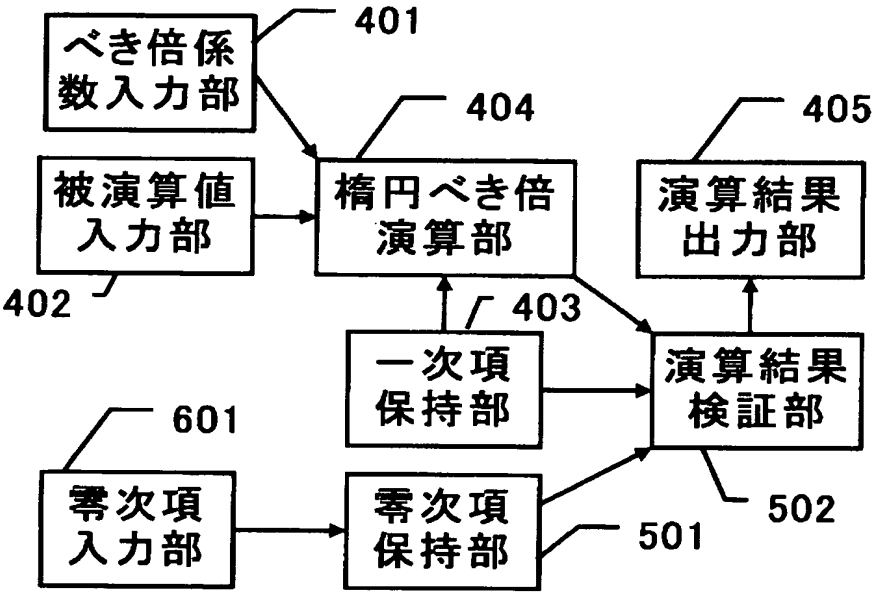
【図４】


べき倍係数入力部
401
404
405
被演算値入力部
楕円べき倍演算部
演算結果出力部
402
403
一次項保持部

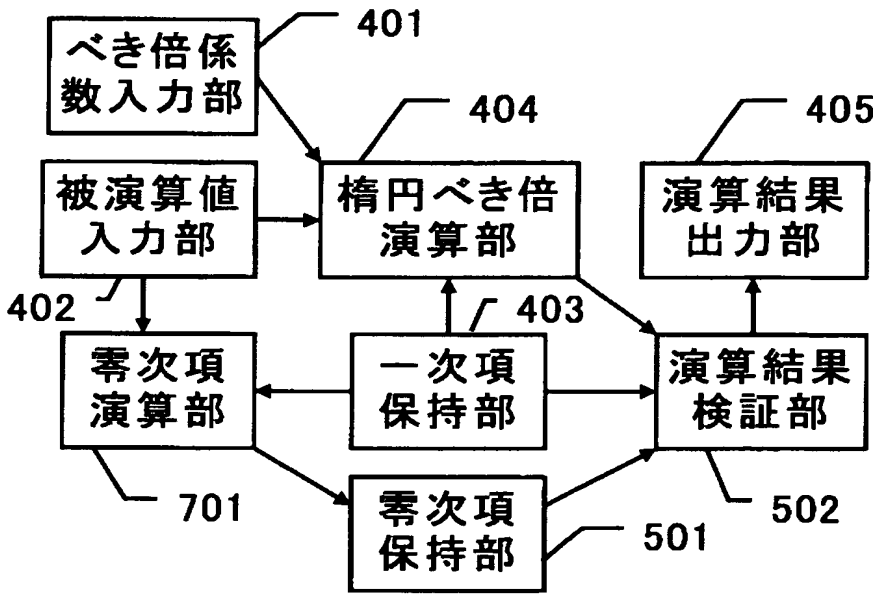
【図５】


べき倍係数入力部
401
404
405
被演算値入力部
楕円べき倍演算部
演算結果出力部
402
403
一次項保持部
演算結果検証部
零次項保持部
501
502

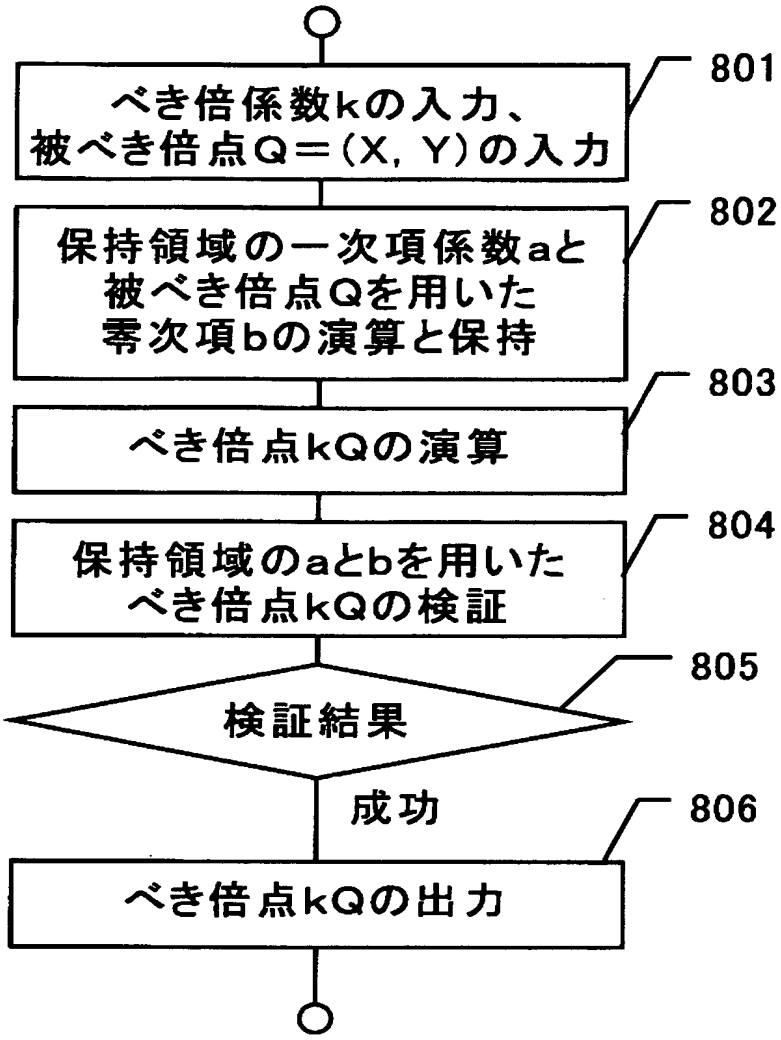
【図６】


べき倍係数入力部
401
404
405
被演算値入力部
楕円べき倍演算部
演算結果出力部
402
403
一次項保持部
演算結果検証部
601
零次項入力部
零次項保持部
501
502

【図７】


べき倍係数入力部
401
404
405
被演算値入力部
楕円べき倍演算部
演算結果出力部
402
403
零次項演算部
一次項保持部
演算結果検証部
701
零次項保持部
501
502

【図８】


べき倍係数kの入力、
被べき倍点Q＝(X, Y)の入力
801
保持領域の一次項係数aと
被べき倍点Qを用いた
零次項bの演算と保持
802
べき倍点kQの演算
803
保持領域のaとbを用いた
べき倍点kQの検証
804
検証結果
805
成功
806
べき倍点kQの出力

【書類名】　要約書

【要約】

【課題】　従来の故障利用攻撃に対応した楕円べき倍演算装置は、使用する楕円曲線のパラメータを固定する必要がある。従ってパラメータを変化させることで異なる暗号となる楕円曲線暗号の汎用性が阻害される。

【解決手段】　楕円曲線のパラメータ零次項係数ｂを入力する手段を設ける。もしくは楕円曲線のパラメータ一次項係数ａ、並びに入力された被べき倍点Ｑから零次項係数ｂを計算して保持する。こうして得られた値を故障利用攻撃に対応するためのべき倍点ｋＱの検証に使用する。

【選択図】　図７

特願２００３－０１８７６０

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社